MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY) END SEMESTER EXAMINATIONS, JUNE 2022

SUBJECT: CRYPTANALYSIS [CSE 5271]

REVISED CREDIT SYSTEM
(23/06/2022)

Time: 3 Hours MAX. MARKS: 50

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data may be suitably assumed.

1.A Bob and Alice decide to communicate using RSA Algorithm. Alice computes the private key with public modulus N= 1537, and public key e=7 and transmits the public parameters to Bob. Eve intercepts the communication and uses the Quadratic Sieve Algorithm in order to cryptanalyze the cipher. Show the steps followed by Eve. **5M**

1.B Show that Diffie-Hellman key exchange algorithm is not secure against the following attacks **3M**

(i) Active attacks
(ii) Man in the middle attack

1.C Do you think that bit slicing can be used as a technique for improving the speed of cryptanalysis of DES cipher? Support your answer with suitable explanation. **2M**

2.A Using Index Calculus method of finding Discrete logarithm find x in $a^x = b \pmod p$ given a=2, b=10 and p=19. Clearly indicate all the steps in the computation. **5M**

2.B Show that Delayed CBC encryption as a block wise mode of operation is (slightly) more vulnerable to attacks beyond the birthday paradox bound than ordinary CBC encryption used as a message wise mode of operation. **3M**

2.C Using Baby step Giant step algorithm , compute x in 3^x =19(mod 59) **2M**

3.A Consider SHA0 hashing algorithm. Introduce a change on single bit of W and let the change occur in the 3rd bit position. Summarize all possible interactions between interleaved local collisions and list them in a table. How many interferences of overlapping local collisions are identified? Explain. **5M**

3.B Consider an Elliptic curve given by the expression $y^2 = x^3 + x - 1 \pmod N$ with a point P(1,1) on the elliptic curve. Compute the factors of N, where N=21, using Lenstra’s elliptic curve factorization method. Clearly show all the steps. **3M**

3.C Show that CBC MAC is not secure for varying length messages. **2M**

4.A Describe Floyd’s and Brent’s cycle detection algorithms and bring out a comparison of both. Identify which one is better and why? **5M**

4.B Identify the type of cryptosystem on which 'sliding attack' could be performed. Describe how 'sliding with a twist' attack is performed, with necessary diagrams **3M**

4.C RSA is a public key cryptographic algorithm. Is it possible to subject RSA algorithm to birthday attacks? If yes, state the requirements and elaborate the process. If no, mention the reasons. **2M**

5.A Using Atkin and Bernstein's sieve, compute the prime numbers less than 60. Clearly indicate all the steps. **5M**

5.B Suppose Bob uses RSA algorithm to encrypt a message using the public modulus 899 and public key 7. Show how Pollard's (p-1) algorithm can be used to attack the RSA cryptosystem. Clearly indicate all the steps. **3M**

5.C For the given function $F(x) = (x^2 + 1) \pmod{255}$, with initial value for x as 3, find the length of the cycle and the tail. Plot the function. **2M**